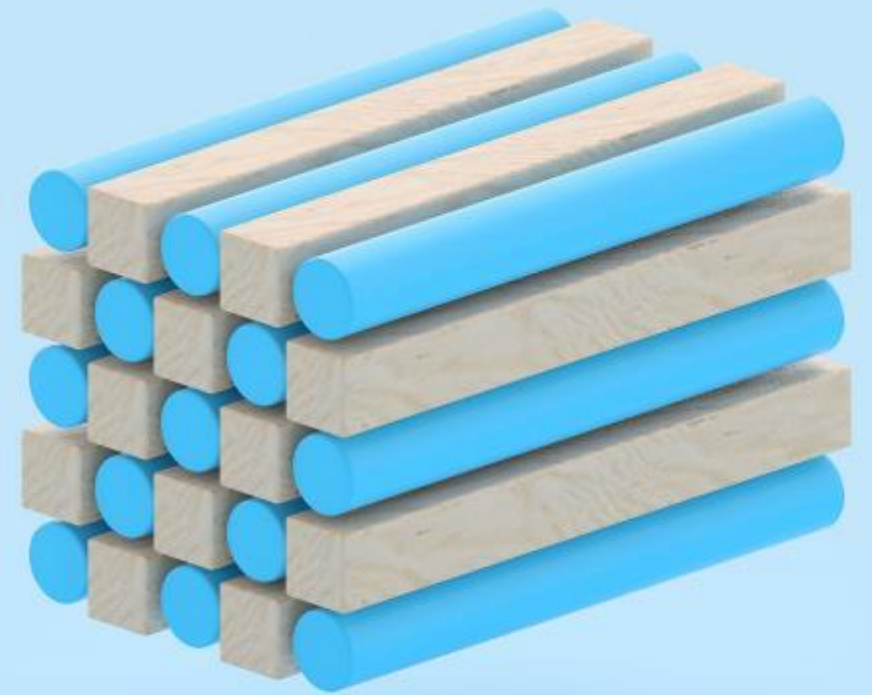


NetApp Tech Community ONLINE

ネットアップ合同会社

2023/5/30



NetApp Tech Community ONLINE

- NetApp SE主催のオンラインセミナー

- 全国のお客様、パートナー様を対象に毎月開催します！
- データ管理を軸とした、最新技術情報、ユースケース、事例、検証結果など
 - DX, AI, ハイブリッド・マルチクラウド, コンテナ, セキュリティ, 災害対策, HCI, オールフラッシュ, Windows 10 VDI, etc

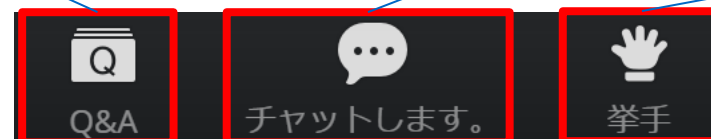
- Zoom Webinarを使ったオンラインセミナー

- PC, スマートフォンの様々なデバイスからお手軽にご参加が可能
- チャット、Q&Aツールの利用による双方向型のコミュニケーション
- オンデマンドであとから録画を確認することも可能

Zoom Webinarセッションの機能

Q&A

- ご質問がございましたら Q&Aをクリックし、ご質問内容を入力後に送信をクリックください
- ホストとパネリストが内容を確認してできる限りセッションの中で回答いたします
- チャット、挙手の機能は通常使用しません



本日のテーマ

NetApp Tech Community ONLINE Vol.40

SaaSベースでお手軽導入！でもネットワーク要件の厳しいオンプレにも対応！ NetAppのクラウドバックアップサービスでオンプレ・クラウドのONTAPに格納されたデータを万全に保護しましょう！

ランサムウェア攻撃、情報漏洩、悪意あるユーザーによるオペレーション、など数え上げたらキリがないほど、様々なリスクにさらされている昨今のビジネス環境で、DX化、IT環境のモダナイズ化に伴い、ハイブリッド・マルチクラウドの環境が浸透し、利便性が向上する一方、データやワークロードが分散化してしまい、データの価値が高まるもそれを狙う攻撃や漏洩のリスクは高まる一方です。

昨年から大幅にアップデートされてきたNetAppのクラウドバックアップサービス（CBS）を活用し、ネットワーク環境の厳しいオンプレミス環境（ダークサイト）などのオンプレやクラウドのONTAPに分散するお客様のデータを万全に保護するソリューションをご紹介します。



スピーカー:

ネットアップ合同会社
Partner Technical Lead
比良 俊也



ネットアップ SE
タナケン



ネットアップ CSM
ドン

BlueXP backup and recovery のご紹介



ネットアップ合同会社 パートナーSE部
パートナーテクニカルリード 比良 俊也
2023年5月30日



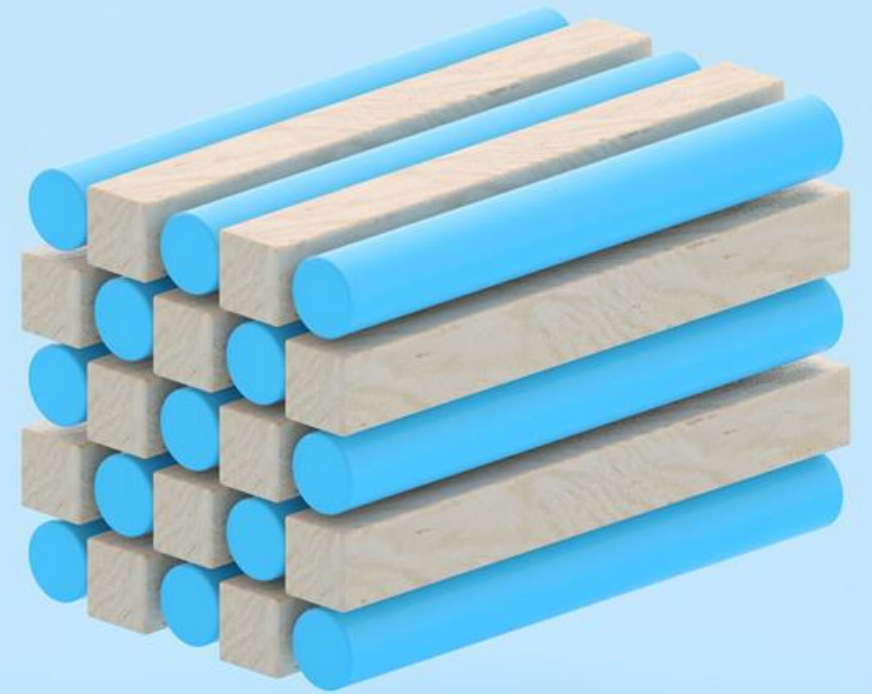
目次



- はじめに
- BlueXP backup and recoveryの紹介
 - クラウドベースのバックアップサービスの提供価値
 - BlueXP backup and recoveryの概要
 - 主要機能のご紹介とデモ
 - ライセンスの考え方について
- まとめ

クラウドベースのバックアップサービスの提供価値

SaaSベースのバックアップサービス

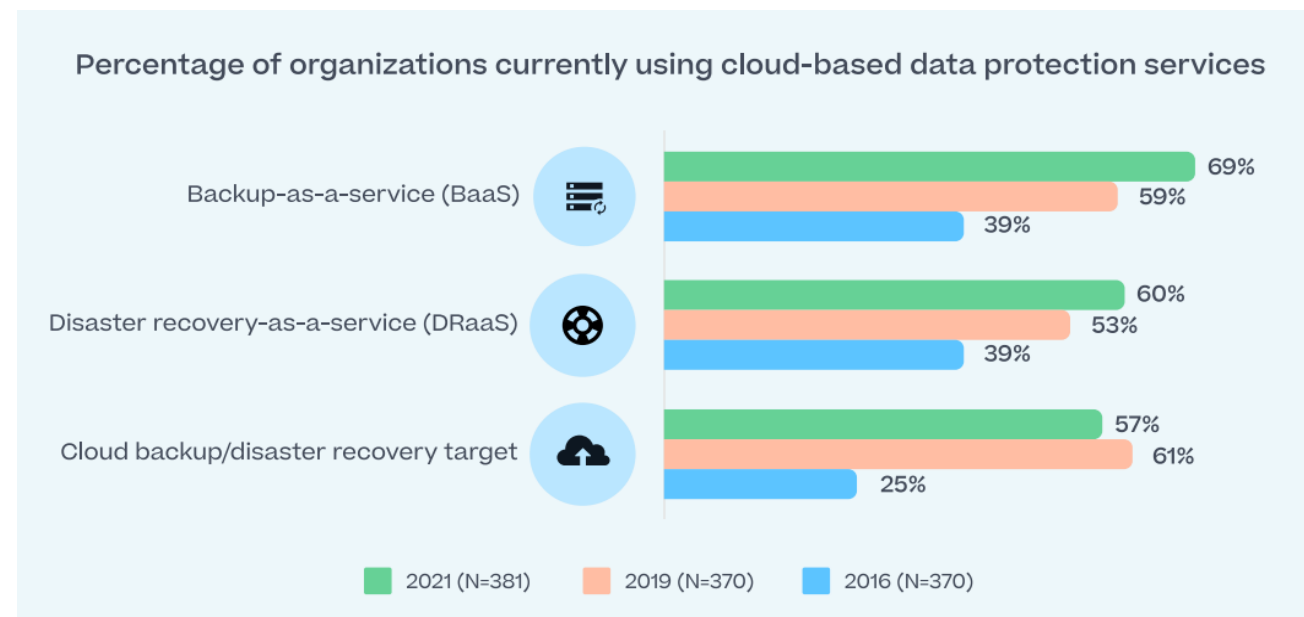


従来のバックアップからSaaSバックアップへ

従来のバックアップでの課題解決のためクラウドを利用したSaaSバックアップ(BaaS/DRaaS)への移行がトレンドとなっている

- BaaSの使用率推移
 - 2016年：39%→2021年：69%
- DRaaS使用率推移
 - 2016年：39%→2021年：60%

一般的なトレンドとしてクラウドをバックアップ/DRのターゲットとして利用している企業は25%から57%に増加している



ソース：Enterprise Strategy Group：[The Evolution of Data Protection Cloud Strategies\(2021\)](#)

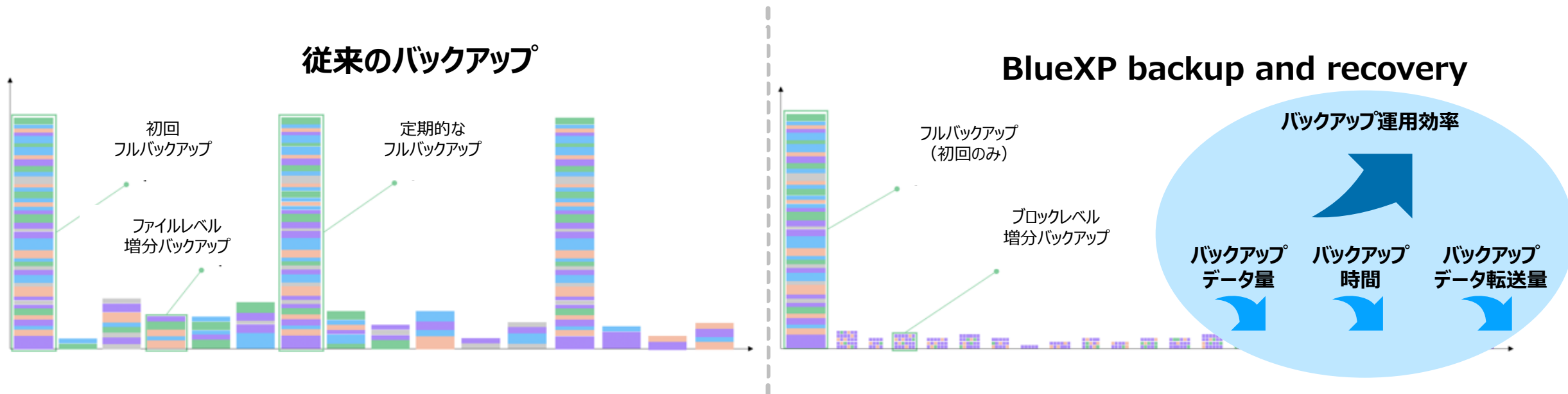
ファイルレベル 対 ブロックレベルのバックアップ

	ファイルレベル	ブロックレベル
効率性 	ファイルレベルではONTAPの効率性が悪くなる →バックアップ対象データが増える→ 時間がかかる	ブロックは効率性を維持
性能性 	ファイルレベルではストレージの全体スループットが低下し →本番環境に影響を与える可能性がある	ブロックでは高速で、本番環境への影響も少なくなる
信頼性 	ファイルレベルの信頼が低い (開き中ファイル、権限、チェックサム)	ブロックではバックアップの信頼性が高い
SLA 	ファイルレベルでは非常に長くバックアップ期間は必要ため、 リスクにさらされる可能性がある	ブロックレベルでは永久に増分となるため、 RPO/RTOを満たす

BlueXP backup and recovery vs 3rd party バックアップソリューション

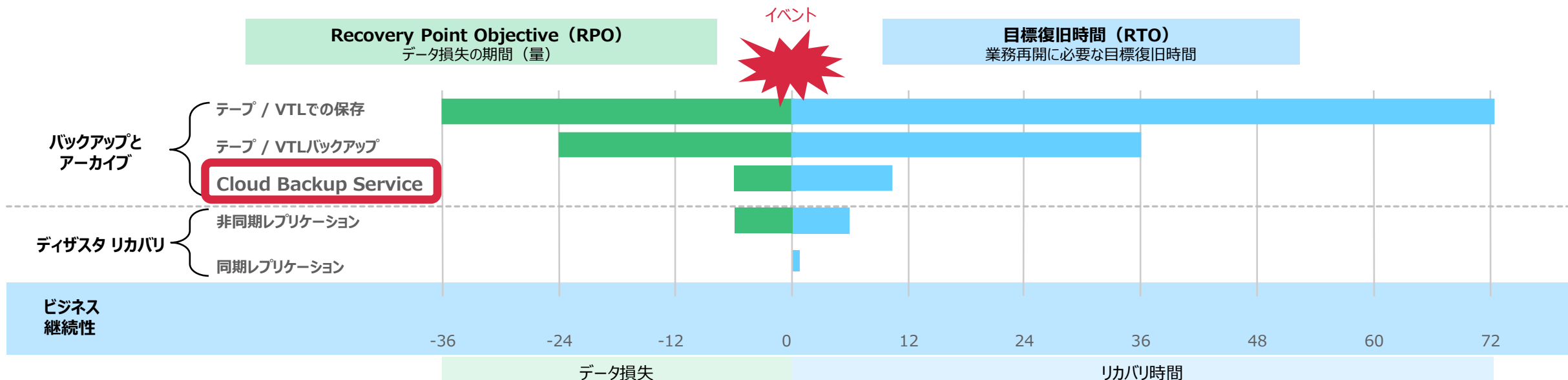
ブロックレベル永久増分バックアップ vs 従来のバックアップ

- 大容量化が進むストレージシステムにおいて、**定期的にフルバックアップ**を実行する時間の確保は困難
- **初回のみ**のフルバックアップに加え、**ブロックレベルの増分バックアップ**により、従来のソリューションに比べ、**大幅なデータ転送量の低減を実現**
- 大容量ストレージシステムにおいても**理想的なバックアップ運用を実現可能**



BlueXP backup and recovery vs 災害対策（DR）ソリューション

許容できるPROとRTOで使いどころを考える



BlueXP backup and recovery

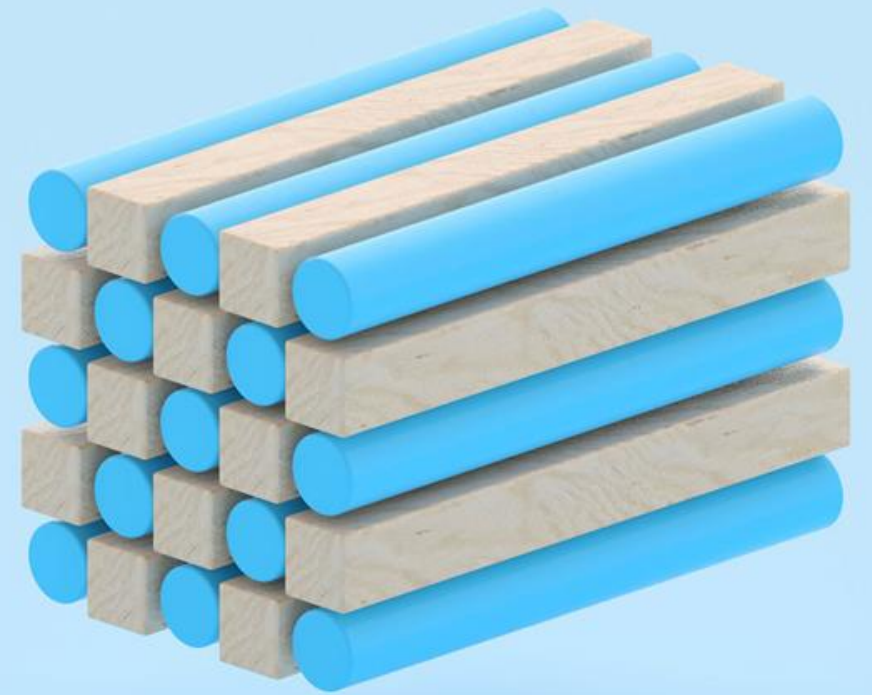
- RPO（1時間～） / RTOはデータ量依存
- データを使えるようにするにはリストアが必要
- 障害復旧後もバックアップデータは残り
バックアップ運用も継続可能
- バックアップデータの改ざんは原則不可能

災害対策（DR）

- 数時間～数分のRPOとRTO
- DR先をプライマリにスイッチして利用
- 障害復旧後も災害対策を講じるには
切り戻しを行うか別のDR先を用意する必要がある
- プライマリへの切り替え後はそれまでの状態が失われるため
アーカイブ用途には不向き

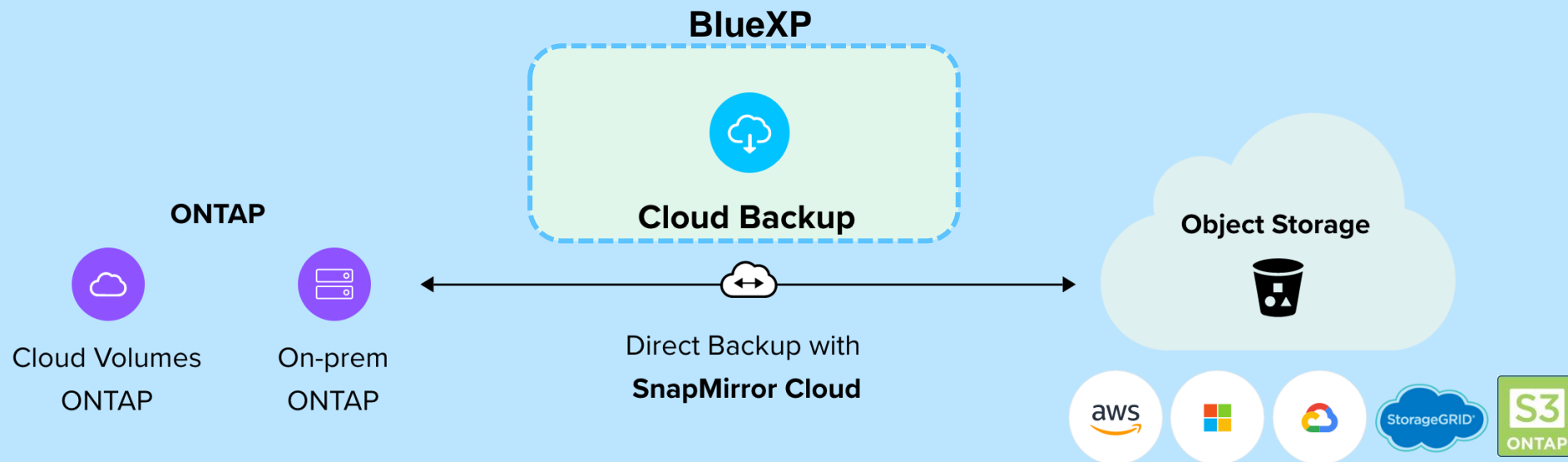
BlueXP backup and recovery の概要

機能の特徴とアーキテクチャ



BlueXP backup and recovery

ONTAP向けに設計されたNetAppのNativeバックアップサービス



- BlueXPからSaaSとして提供(DarkSiteにも対応)
- SnapMirror Cloud とのオーケストレーション
- 外部ツール不要
- バックアップの専門知識は不要
- 完全に自動化され、API駆動型ストレージ効率を維持した状態でのブロックレベルバックアップによるバックアップ高速化

BlueXP backup and recoveryの概要

Cloud Volumes ONTAPやオンプレにあるONTAP上のデータを、手軽にクラウドやオンプレのオブジェクトストレージへバックアップ

NetApp BlueXPに統合

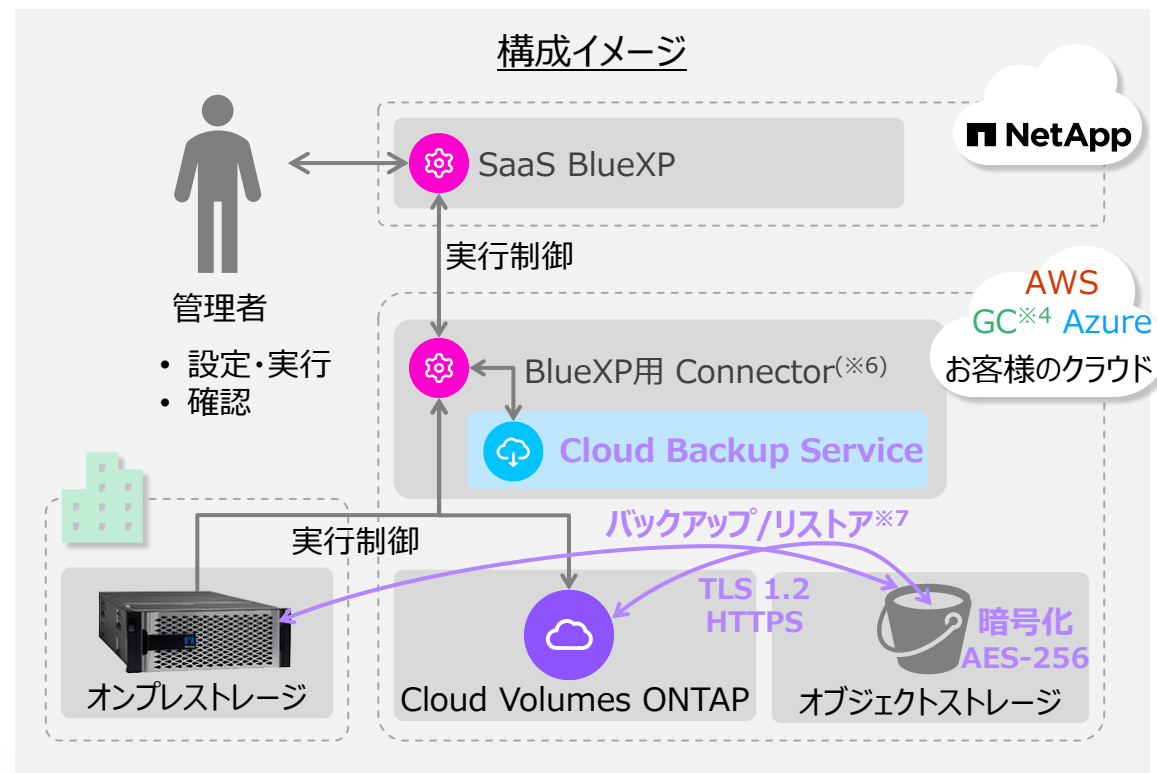
- BlueXPによりバックアップを自動化。(API対応)
- 他のツールやバックアップの専門知識は不要、手軽に導入・運用可能。

バックアップ・リストア機能を提供するアドオンサービス

- CVOやオンプレミスのONTAPストレージ上のデータを、クラウド上やオンプレミスのオブジェクトストレージに、独立した状態でバックアップ。(※1)
- 最もシンプルなバックアップソリューション
 - ポリシーベースのバックアップ操作とバックアップはブロックレベルの永遠増分
- ボリューム単位のバックアップを、ブロックレベルで迅速・効率的に実現。
 - ✓ ONTAPの“SnapMirror Cloud”(※2)の機能を利用。
- ボリューム、フォルダ、ファイルレベルでリストア可能。(※3,4)

バックアップデータはクラウド上やオンプレのオブジェクトストレージに格納(※1)

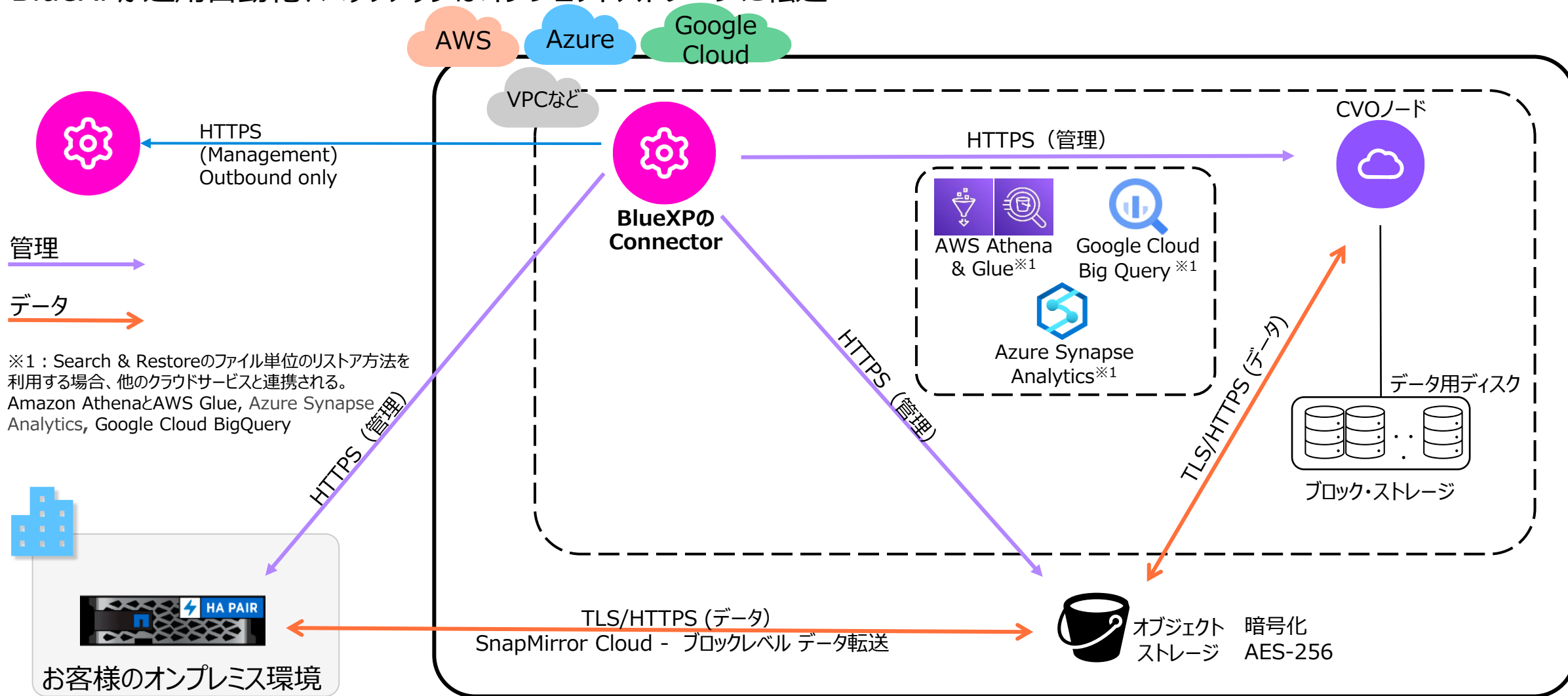
- お客様所有のオブジェクトストレージに格納。
 - ✓ AWS, Azure, Google CloudとStorageGRIDも対応。(※3,4,5)
- 完全に暗号化、保管時(AES-256)・転送時(TLS1.2/HTTPS)ともに保護。



- ※1：オンプレミスのオブジェクトストレージはStorageGRIDです。(利用可能はオンプレミスのONTAPのみ)
- ※2：SnapMirrorの拡張機能。ONTAPのスナップショットコピーをオブジェクトストレージに転送。
- ※3：ファイル単位でのリストアの機能名はBrowse & Restore又はSearch & Restore。両方オンプレのONTAPと同じクラウドのCVOへリストア可能。(詳細)
- ※4：クラウドによる状況は異なる可能性がある。(一般制限事項の詳細)
- ※5：オンプレからオンプレまでで行う場合はオンプレのConnector、BYOLとStorageGRIDは必要。
- ※6：Search & Restoreのファイル単位のリストア方法を利用する場合、他のクラウドサービスと連携される。Amazon Athena, AWS Glue, Google Cloud BigQuery (詳細)

【アーキテクチャ】 Cloud Volumes ONTAP / オンプレONTAPのいずれにも対応

BlueXPが運用自動化、バックアップはオブジェクトストレージに転送



対応しているプラットフォーム

対応しているプラットフォームとStorage及びCloud BackupでサポートしているWorkload

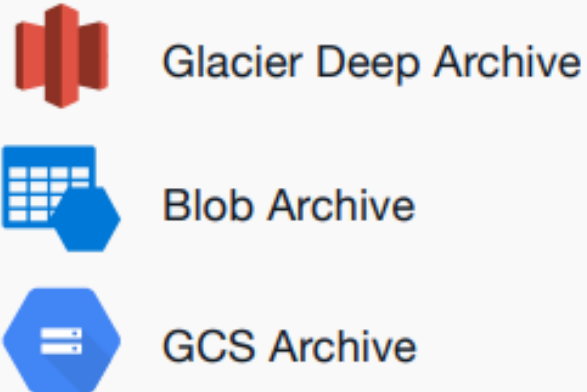
Availability



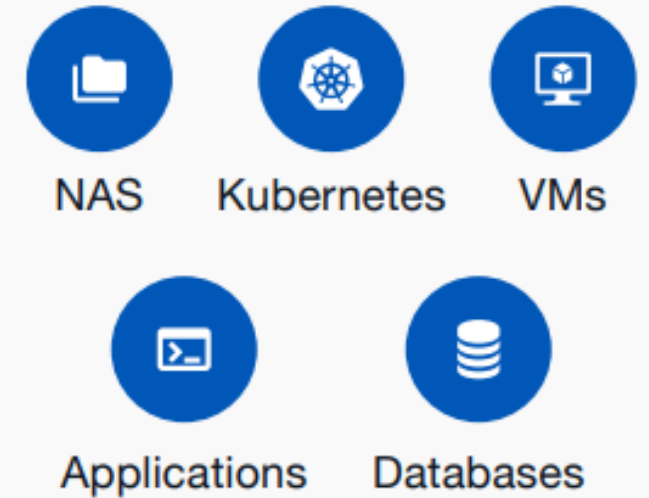
- All major cloud providers
- SaaS or self-managed SW
- All cloud regions
- Gov Cloud

Archival tiers

Utilize the lowest-priced storage with cloud archival tiers.



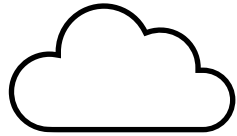
Supported workloads



※Application/Databases/VMはSnapCenterとの連携が必要
対応データベース/アプリケーション(2023年05月30日現在)

- Oracle & SQL
- VMWare
- SAP HANA

BlueXP backup and recoveryの主なユースケース



クラウドバックアップ & アーカイブ

- バックアップは独立した個別コピーです。（スナップショットはボリューム内の変更ブロックの増分のみ保持する仕組み）
- オフサイト（ストレージ外）にバックアップすることで、「3-2-1バックアップ戦略」^(※1)を実現
- オンプレミスのONTAP上のボリュームを削除・消失した後も必要に応じて取り出し可能な、長期アーカイブとしても活用可能



災害からのリカバリ

- 一次データとは別の場所（オブジェクトストレージ）
- 同じリージョンのCloud Volumes ONTAPにリカバリ可能
- クロスリージョンのバックアップとリストア提供予定



ランサムウェア保護

- バックアップは読み取り専用のため、変更不可。
- 内部犯の脅威や偶発的な削除からデータを保護。



モダナイゼーション

- 従来のテープソリューションの置き換え。
- 古くなってきているローカルバックアップ先をクラウドと更新。

※1：データはオリジナル1つと2種類のバックアップを作成し（合計3つ）、2種類のバックアップのうち1つはオフサイト（クラウド等）に保管する、というバックアップ戦略。

バックアップで実現するバックアップ戦略

3-2-1ルール

3

データ
コピー

追加のデータコピー作成

2

メディア
タイプ

オブジェクトストレージへの
フォーマット変更

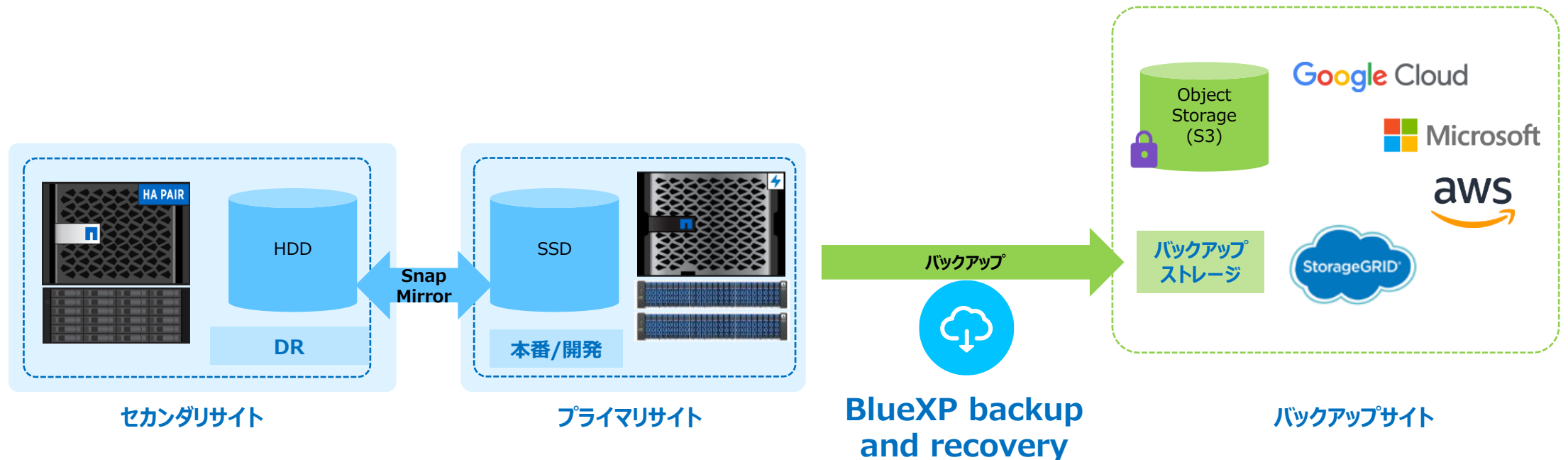
1

オフサイト
コピー

オフサイトにコピーを保存

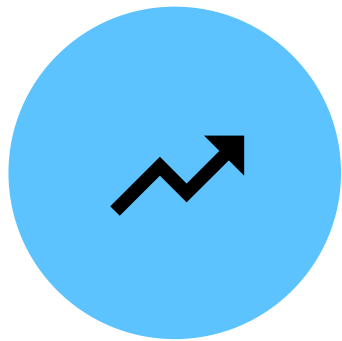
ネットアップで実現する3-2-1バックアップ戦略の概要

- 3 – 2 – 1 ルールに即したバックアップ
 - 3 データを3つ：セカンダリサイト(SnapMirror)とバックアップサイトにコピー
 - 2 つ以上の媒体：ONTAP(WAFL)とS3
 - 1 つのオフサイト：Cloud Backupでエアギャップ(書き換え不可能なバックアップ)を実現



提供価値

ONTAPの優れた機能を活用した、クラウドへのバックアップ機能をご提供



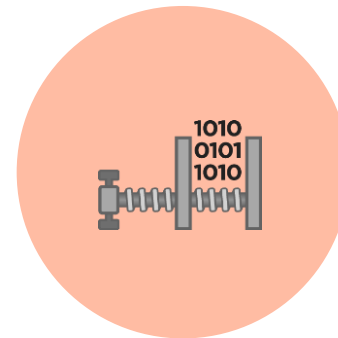
簡単操作



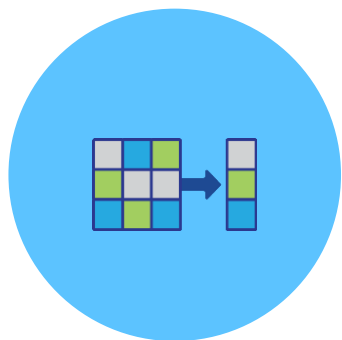
永久に増分のみ



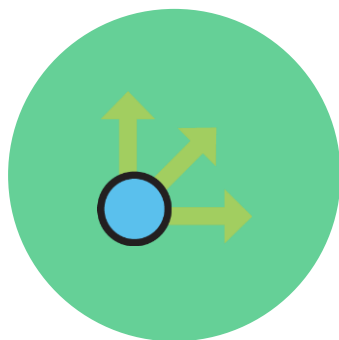
高い信頼性
(ブロックレベル)



データセンターの
設置面積削減



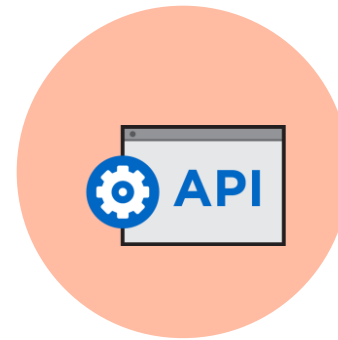
ストレージ効率性を維持
(圧縮、重複排除等)



無制限なスケーラビリティ

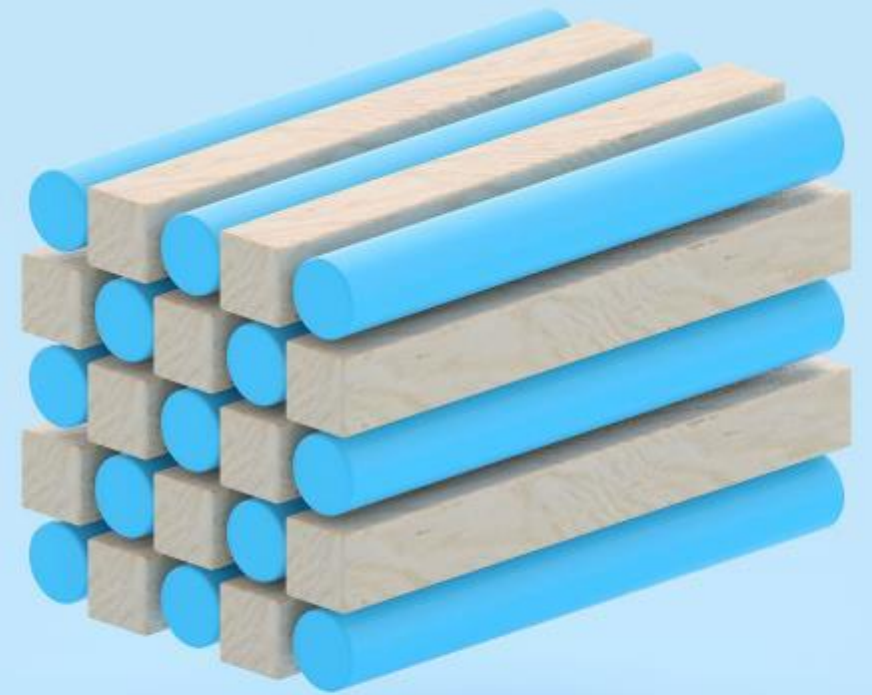


瞬時に細かな粒度での
リストア



API駆動サービス
(簡単な自動化)

BlueXP backup and recovery 主要機能のご紹介



BlueXP backup and recoveryの主要な機能のご紹介

バックアップデータの
保護

Ransomware protection

整合性を保持した
データ保護

Application / VM

リスト対象のファイル
特定

Search and Restore

長期間低コストで
データを保管

All clouds archive

ネットワーク要件の
厳しい環境に対応

Private cloud backup

きめ細やかな粒度
でのリストア

Granular restore

情報セキュリティ10大脅威 2023

「ランサムウェアによる被害」が3年連続で「組織」向け脅威の1位に

順位	「組織」向け脅威	前年順位
1位	ランサムウェアによる被害	1位(-)
2位	サプライチェーンの弱点を悪用した攻撃	3位(↑)
3位	標的型攻撃による機密情報の窃取	2位(↓)
4位	内部不正による情報漏えい	5位(↑)
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位(↓)
6位	修正プログラムの公開前を狙う攻撃 (ゼロデイ攻撃)	7位(↑)
7位	ビジネスメール詐欺による金銭被害	8位(↑)
8位	脆弱性対策情報の公開に伴う悪用増加	6位(↓)
9位	不注意による情報漏えい等の被害	10位(↑)
10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

- 3年連続で「**ランサムウェアによる被害**」が1位
- 情報の暗号化のみならず、窃取した情報を公開すると脅す「**二重脅迫**」に加え、DDoS攻撃を仕掛ける、被害者の顧客や利害関係者へ連絡するとさらに脅す「**四重脅迫**」が新たな手口として挙げられている
- **RaaS (Ransomware as a Service)**などの流行もあり、2022年は圏外だった「犯罪のビジネス化（アンダーグラウンドサービス）」がランクイン

バックアップデータに対するランサムウェア対策機能を強化

バックアップデータのロック機能

- 一定期間、バックアップファイルが変更または削除されないようにするというData Lock機能が追加。
- 設定された通常のバックアップ+14日間の設定で機能 (最小30日の期間を要するため、 $30+14 = 44$ 日のロックが最小)

ランサムウェアスキャン機能

- バックアップファイルをスキャンすることで、ランサムウェア攻撃の有無を検出
- スキャンのタイミングはバックアップ実施時、リストアの実施時、手動の3種
- 検出された場合、非検出と思われるバックアップファイルに最新バックアップが置き換えられる
(1日後に検出されたバックアップは削除)

DataLock & Ransomware Protection

Backup copies are protected from being modified or deleted, and they are scanned for ransomware threats.

- None
- Governance
Users with specific permissions can overwrite or delete protected backup files during the retention period
- Compliance
No users can overwrite or delete protected backup files during the retention period

DataLock & Ransomware Protection Information

- DataLock protection mode can't be changed after the policy is created
- Each backup file will be locked during the retention period as defined above, or for a minimum of 30 days, plus a buffer period of up to 14 days. [Learn more.](#)
- Ransomware detection scans are run automatically on each protected backup copy: once during the retention period, and again before a restore operation. You can run detection scans on demand as well.

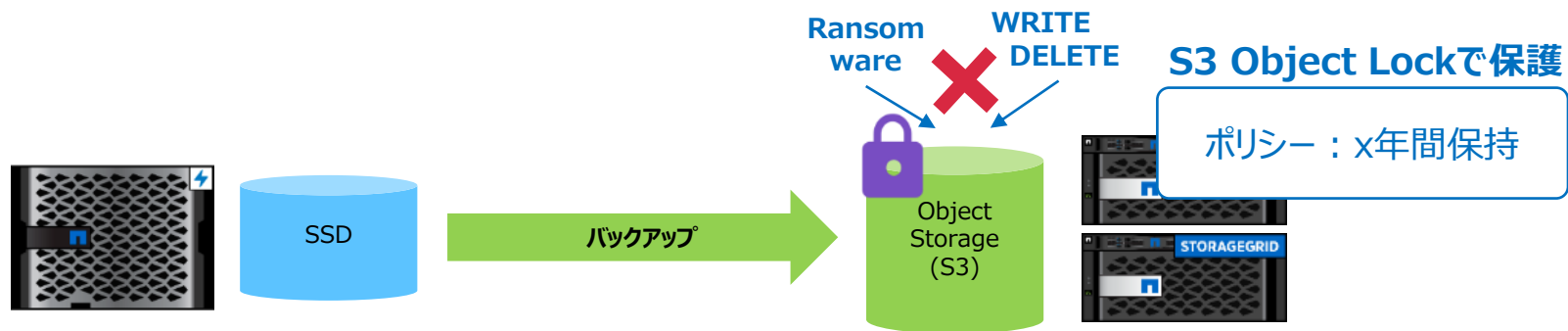
※サポート情報 : AWS : ONTAP 9.11.1, Azure : ONTAP 9.12.1 (オンプレ、CVO) / サポートターゲット: AWS S3, Azure Blob, StorageGRID / 導入環境: SaaS, Dark Site

※参考 : <https://docs.netapp.com/us-en/cloud-manager-backup-restore/concept-cloud-backup-policies.html#datalock-and-ransomware-protection>

書き換え不可能なバックアップとデータの完全性

DataLock機能 – ランサムウェア攻撃、悪意あるファイル操作、ヒューマンエラーによる削除から保護

- S3ストレージに書き込まれたオブジェクトに適用される**WORM機能**(Write Once Read Many)
- 指定された期間、対象の**オブジェクトの変更、削除を禁止し、改ざんを防止**



- SEC 17a-4(f), CFTC Regulation 1.31, FINRA Rule 4511の各規制に準拠
 - S3 Object Lockは電子ストレージメディアでレコードを確実に保持するため、指定した期間レコードの変更・消去を防止するための機能
 - Cohasset Associatesによって評価済み(評価レポート: <https://d1.awsstatic.com/r2018/b/S3-Object-Lock/Amazon-S3-Compliance-Assessment.pdf>)
- 2つのモードで保護強度を選択可能

ガバナンスモード

- 権限を持つユーザーはバックアップの可変・削除が可能

コンプライアンスモード

- すべてのユーザーは指定した期間中バックアップの可変・削除が不可能

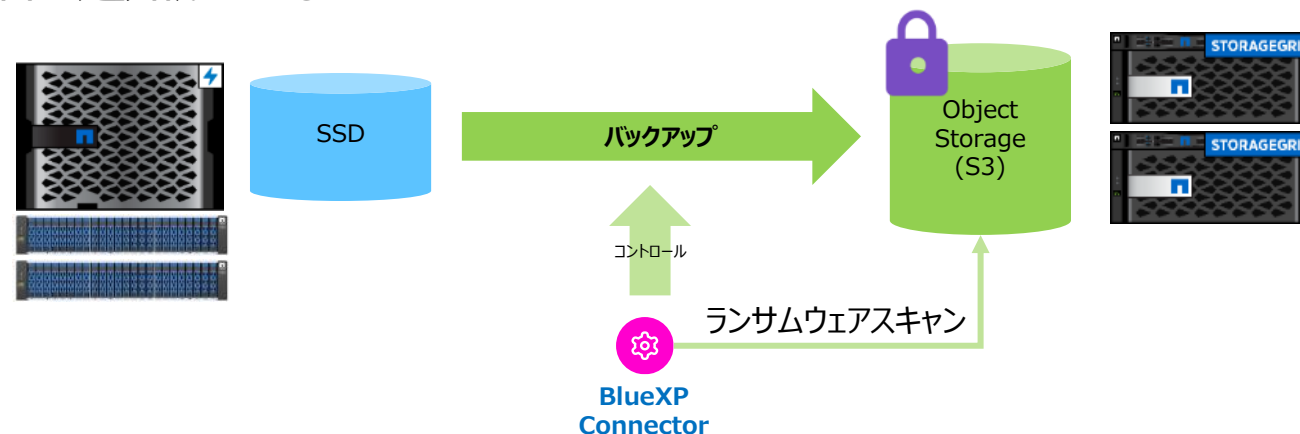
※ StorageGRIDでは2023年5月現在、コンプライアンスモードのみサポート

書き換え不可能なバックアップとデータの完全性

Ransomware Protection機能 – バックアップデータへの攻撃にも万全の対策

- BlueXP backup and recoveryはバックアップデータをスキャンしランサムウェアを検知することが可能
 - バックアップ時
 - リストア時
 - 手動
 - バックアップ元はスキャン対象外

※検知がされた場合、管理者へ通知がされる

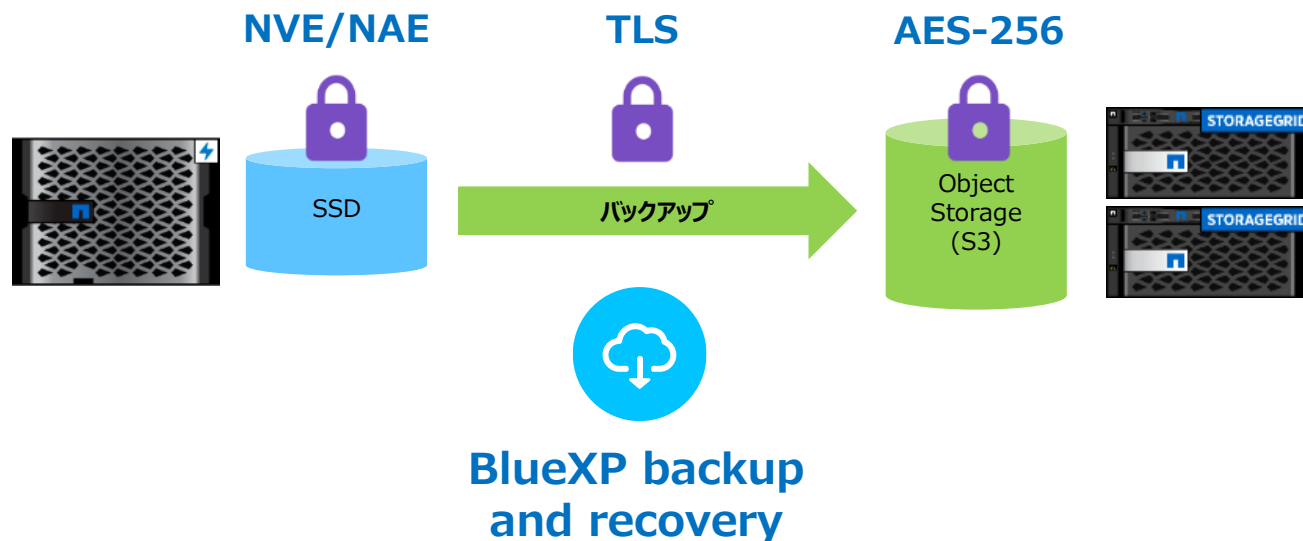


攻撃されたと疑わしいオブジェクトを検出すれば、以前の世代かつクリーンな状態のバックアップされた最新のオブジェクトと置き換えてバックアップデータをクリーンな状態で保持！

※参考：https://www.youtube.com/watch?v=Zy-b8TeXV6Q&list=PLdXI3bZJEw7lwYdptI_7Ipe5i4MQ0apPP

補足:書き換え不可能なバックアップとデータの完全性 バックアップデータの完全性の担保

- バックアップデータの暗号化
 - 暗号化(AES-256)との組み合わせでデータの持ち出しも無効化
 - 通信もTLSで暗号化
 - バックアップ元(ONTAP側)はONTAPのNVE/NAEなどで暗号化



ソース、転送データ、バックアップデータ格納先全ての場所で暗号化を実施して万全に保護！

Backup Volumeを
表示した ページ

Working Environments



Last Updated

June 12 2022, 00:00:00

Backup Settings



2,011

Protected Volumes



125.75 TB

Total Backup Size

Backup Volumes Status



1,924

Healthy Backup Volumes



87

Failed Backup Volumes

2,011 Backed Up Volumes

ランサムウェアの疑いを検出

Source Volume	Source Working Environment	Source SVM Name	Ransomware Protection	Backup Status
Source Volume Name # 1 ● On	Source Working Environment ● On	Source SVM Name	None	● Active
Source Volume Name # 2 ● On	Source Working Environment ● On	Source SVM Name	⚠ Governance	● Active
Source Volume Name # 3 ● On	Source Working Environment ● On	Source SVM Name	⚠ Compliance	● Active
Source Volume Name # 4 ● On	Source Working Environment ● On	Source SVM Name	ⓘ Governance	● Active
Source Volume Name # 5 ● On	Source Working Environment ● On	Source SVM Name	ⓘ Governance	● Active

最後にランサムウェアの
スキャンを
実施した日時

Last Ransomware Protection Scan:
June 12 2022, 00:00:00

Browse and Restore のページ

Ransomware Scan

Ransomware Protection is active for backups from source volume <volumename0123456789>.

Governance	June 12 2022, 00:00:00	Protected
DataLock Mode	Last Scan Date	Last Scan Status

Recommendation

Scan again before restoring

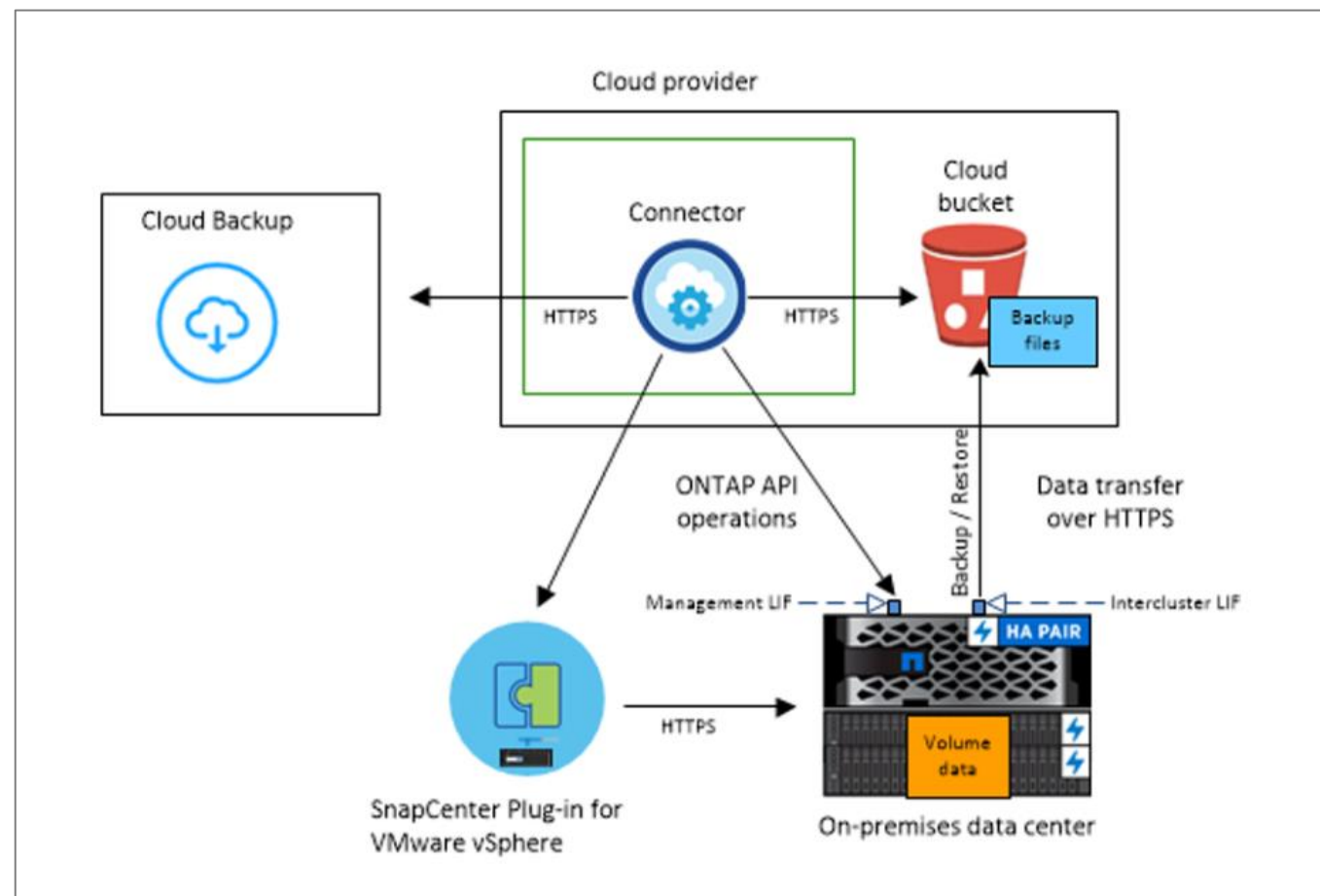
We recommend that you run a ransomware scan before restoring data from a backup file. If the scan identifies a possible ransomware attack, Cloud Backup will automatically revert to the last known good version of the backup copy and complete the restore process.

[Save & Continue](#)

Ransomware Scan	
Protected	
Protected	
Potential Ransomware Identified	
Protected	
Protected	
Protected	
Protected	
Protected	
Protected	
Protected	

SnapCenterとの連携によるアプリケーション / 仮想マシン単位のバックアップ及びリストア

- SnapCenterと連携したデータストアのバックアップ、および個別仮想マシンのリストアに対応 (to S3, Blob, StorageGRID)
- 同一データストアへのリストアに対応 (異なるデータストアへは不可)
- SnapCenterとの統合によるアプリケーションの保護
 - Oracle / Microsoft SQLサーバーの保護
 - オブジェクトストレージへの格納とリストアのサポート



※VMのバックアップ・リストアのイメージ

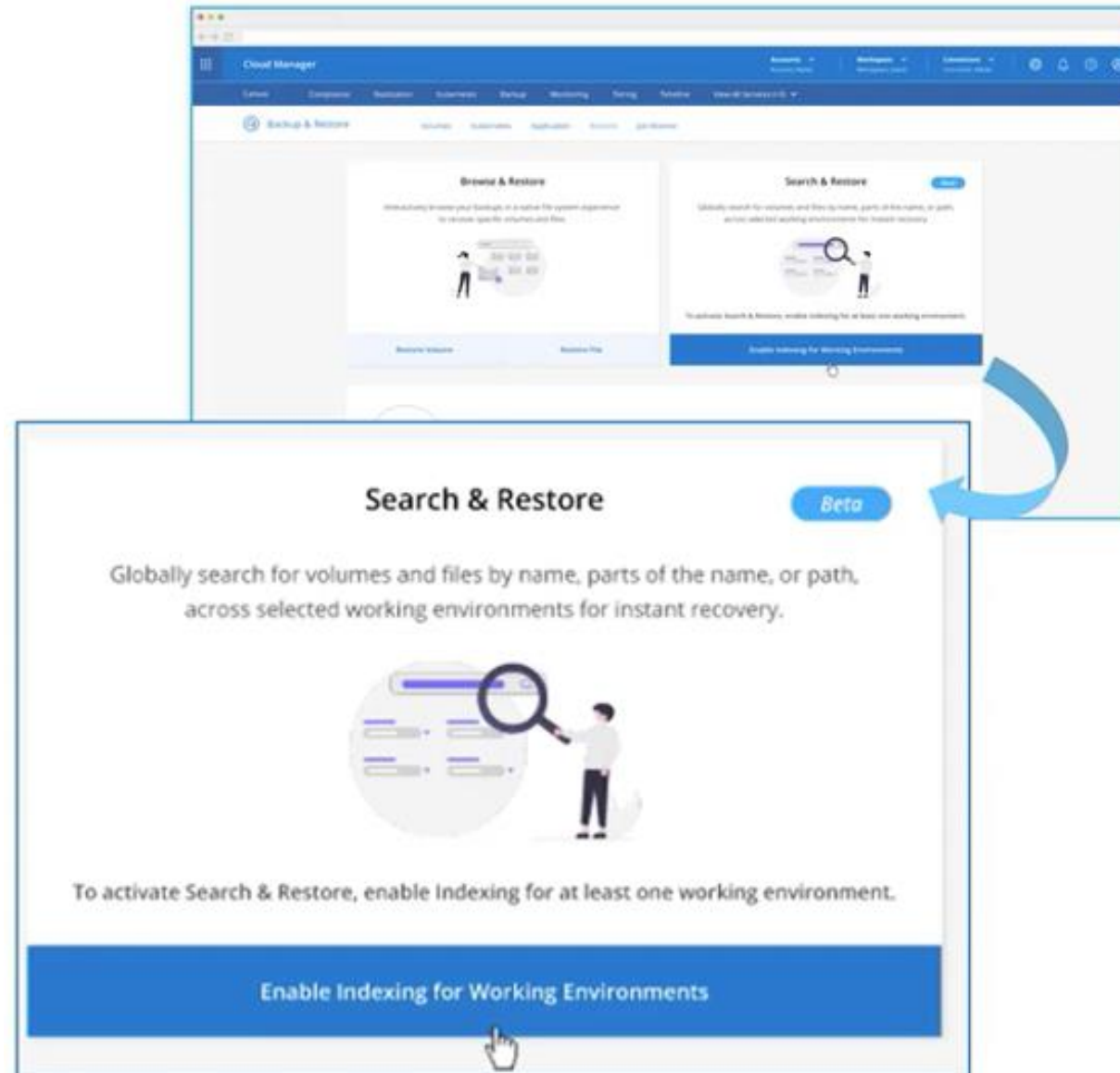
※参考 : <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-restore-vm-data.html>

Indexed Catalog(Search & Restore)

- クラウドストレージに保存されているすべてのバックアップから特定のファイルを検索し、復元を実行可能な「**Indexed Catalog**」を導入
- **クラウド内のすべてのバックアップ**にわたってファイルを**迅速かつ集中的に検索**
- ファイルの簡単で焦点を絞った検索が可能
- **複数の検索条件を使用**するオプションの提供
- SnapDiff v3をベースとし、ファイル・システムを完全に表現
- **ネイティブクラウド技術を使用**して開発
- 新しく作成、削除、名前変更されたディレクトリとファイルを処理

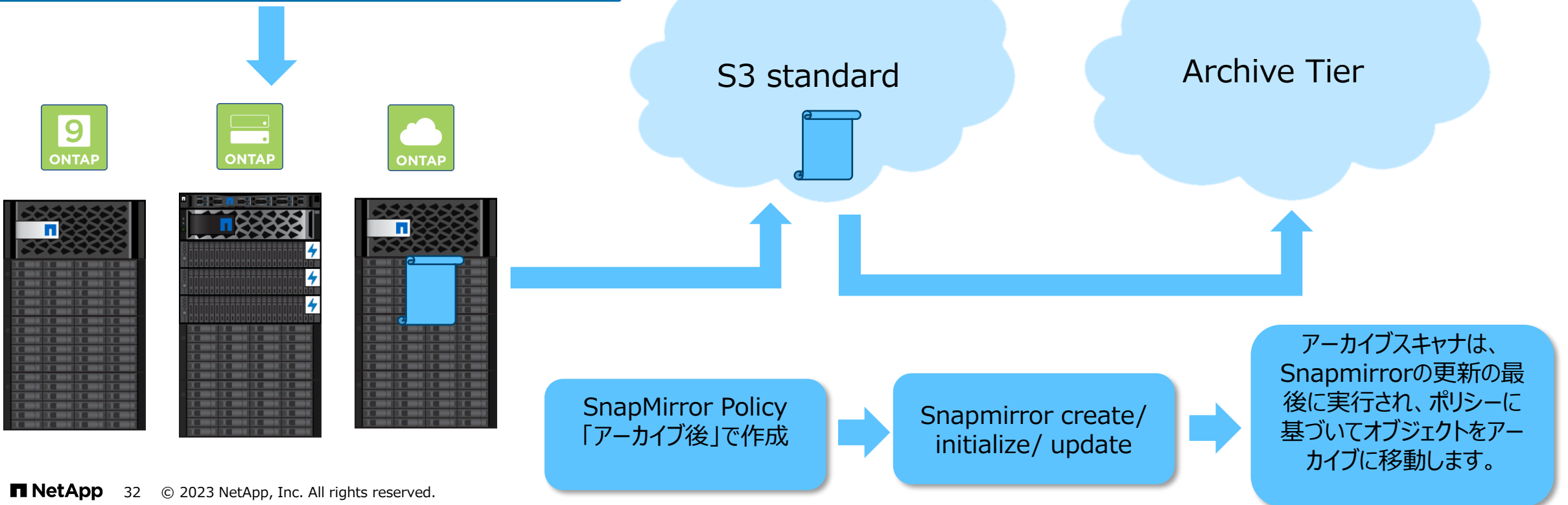
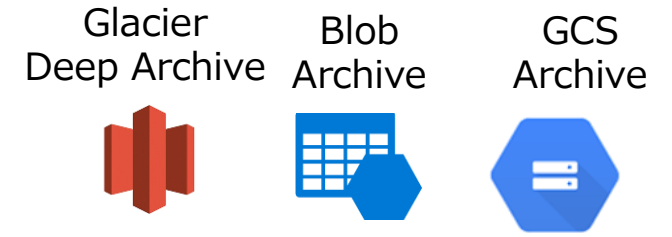
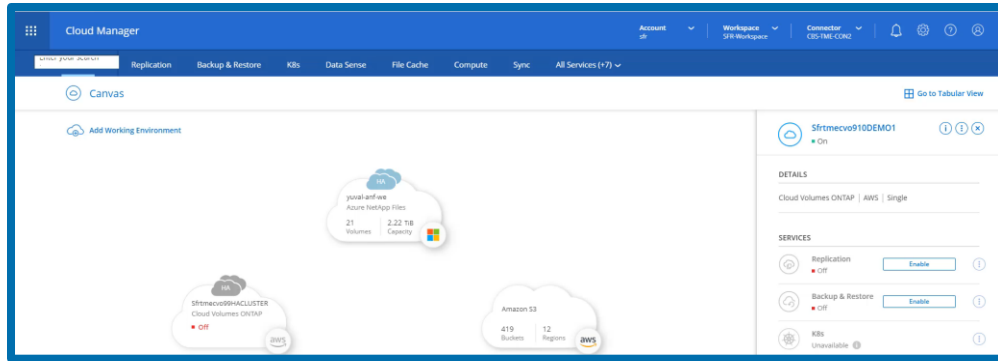
検索基準

- File Name
- File Type
- File Creation Time
- File Size
- Working Environment
- Local & Cloud Backups
- Volume Name



Archive Tierへの対応

- Archive Tiers(version 9.10.1以降)
 - AWS/GCP/Microsoftでサポート
 - Archive, 長期保存 3rd site / コンプライアンス対策目的での利用



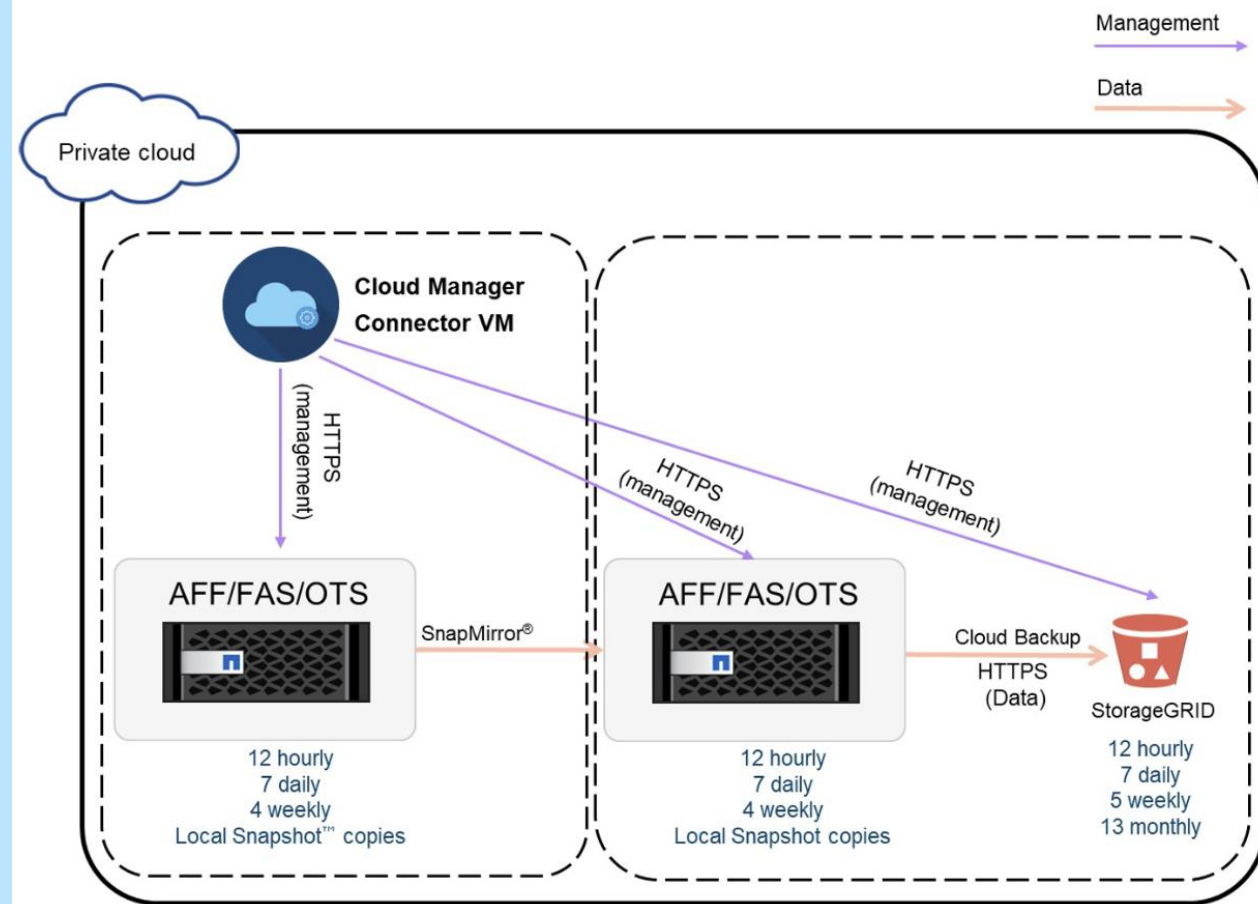
BlueXP backup and recovery: Dark Site Support

インターネットアクセス要件の厳しい環境のバックアップをサポート

- 多くの組織にとって、最高レベルのセキュリティ基準でデータを保護することが不可欠でパブリッククラウドがターゲットとして適さない場合がある
- BlueXP backup and recoveryは、自己管理または「Software-only」モードとして提供されるDark Siteをサポート
- Software-onlyオプションを使用すると、ユーザーはデータを安全に保つための制御をより詳細に制御可能
- データをバックアップするためのアウトバウンドインターネット接続は不要
- コネクタはVMにて立ち上げ
- Indexed Catalog(Search & Restore)をサポート

※Connector Requirements: [Install the Connector on an existing Linux host that has internet access | NetApp Documentation](#)

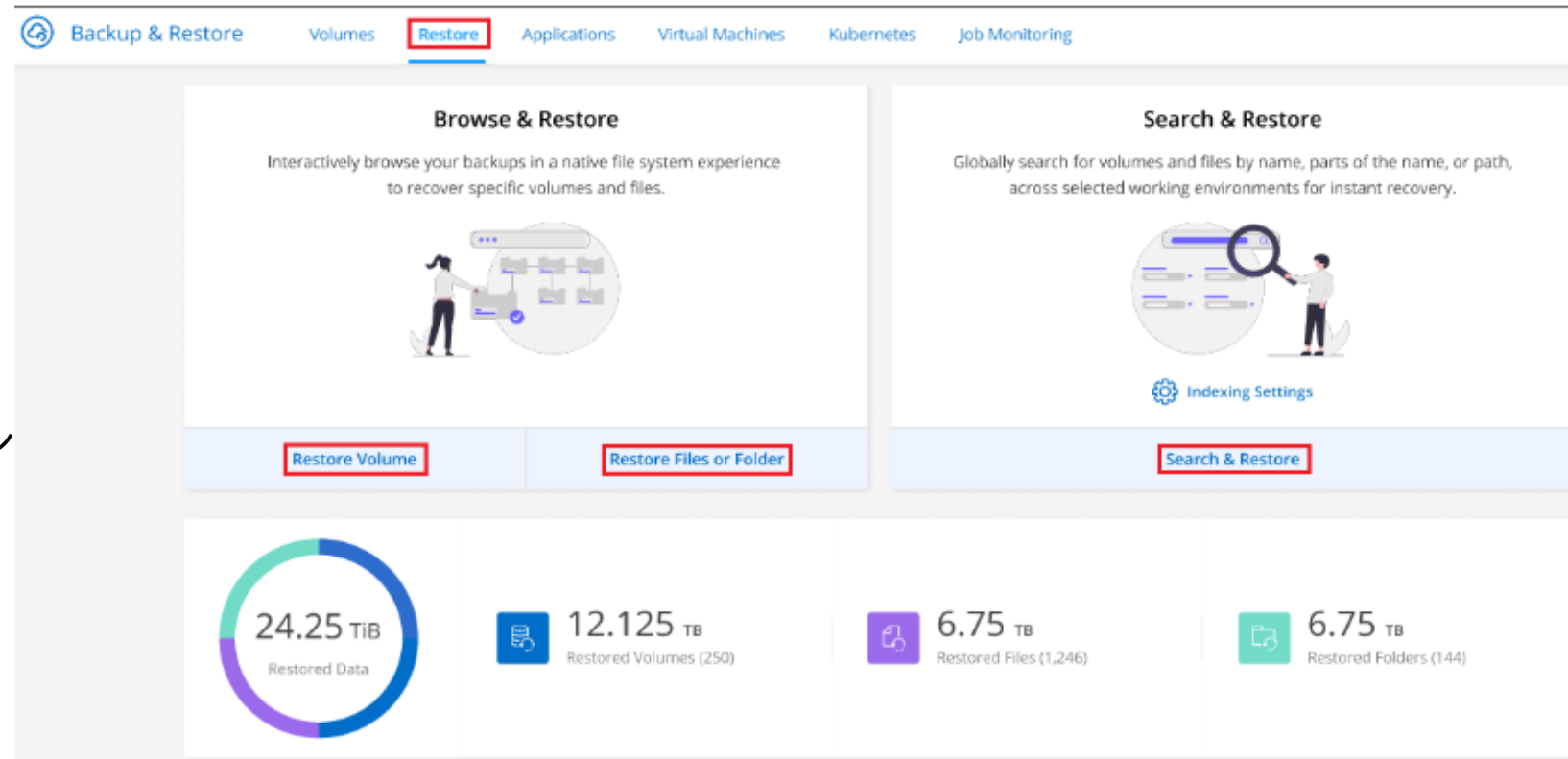
※Indexed Catalog(Dark Site): <https://community.netapp.com/t5/Tech-ONTAP-Blogs/BlueXP-Backup-and-Recovery-Search-and-Restore-Support-for-Dark-Site-Connector/ba-p/440277#toc-hId--846621279>



リストア先は別のONTAPへのリカバリも可能

リストアをきめ細やかな粒度でリストアが可能(Folder Level Restore)

- バックアップからフォルダレベルでのリストアをサポート
- アーカイブストレージに移動したバックアップから個別ファイルをリストアをサポート
- ファイルレベルリストアにおいて、元のファイルを上書きするオプションが選択可能



※参考 : <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-restore-backups-ontap.html#the-restore-dashboard>

BlueXPとの統合で実現するより一層効率的な操作

非常に優秀な効率性

平均

90%

ネットワークトラフィックの現象

より少ないオーバーヘッド

少なくとも

10x

より高速なバックアップ

容易な操作性

最低

2 min

セットアップの時間

シンプルな実効性

たったの

1 click

アクティベーション



1. 選択

Cloud VolumesかオンプレのONTAPクラスタを選択



2. アクティベーション

バックアップ保持期間のポリシーを選択したボリュームに設定



3. 完了

その他の設定は不要

最小の労力で
設定完了！

- ポリシーは毎時、日、週、月又はその組み合わせとシステム定義

バックアップサービス用の CVOシステム定義の ポリシー名	バックアップの間隔			最大 バックアップ
	毎日	毎週	毎月	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

※現在、バックアップの最大はボリュームあたり4,000回です。

※オンデマンドでバックアップを取るも可能です。

- ONTAPのバージョンは9.7P5以上

- AWSは9.6以上、Azureは9.7以上、GCとオンプレは9.7P5以上
- オンプレのシステムにSnapMirrorライセンスが必要

- FlexVolの読み取り/書き込みとデータ保護 (DP) ボリューム

※1: バックアップはセカンダリーONTAPのみ
(MCC→SnapMirror→ONTAP→CBS→オブジェクトストレージ)

- DataLock機能のサポート

オブジェクトストアのWORM/Complianceモードでは、Amazon S3、StorageGRIDのみサポート

※詳細はマニュアルをご参照ください

- 対応可能なオブジェクトストレージ:

- AWS S3→S3-IA、Azure Blob Cool、GC Standard→Nearline以上、GRID
- StorageGRIDはStandardのみ対応
- オブジェクトストレージからのILM (階層化)、またはAWS Glacierまたは同様の下位層のオブジェクトストレージへの直接書き込みは未対応

- 現時点でサポートされていない機能:

- オンプレミスでStorageGRIDへバックアップの場合はクラウドのコネクターは未対応
- SnapLock Compliance ボリュームは未対応
 - SnapLock Enterprise ボリュームはサポート(ONTAP 9.11.1以降)
 - FlexGroupのサポート(9.12.1以降)
- SVM-DRやSM-BC構成とメトロクラスタ (MCC) ※1 は未対応
- StorageGRIDはCVOとの組み合わせは未対応 (オンプレからオンプレのみ対応)

- シングルファイル・フォルダリストアについての制限:

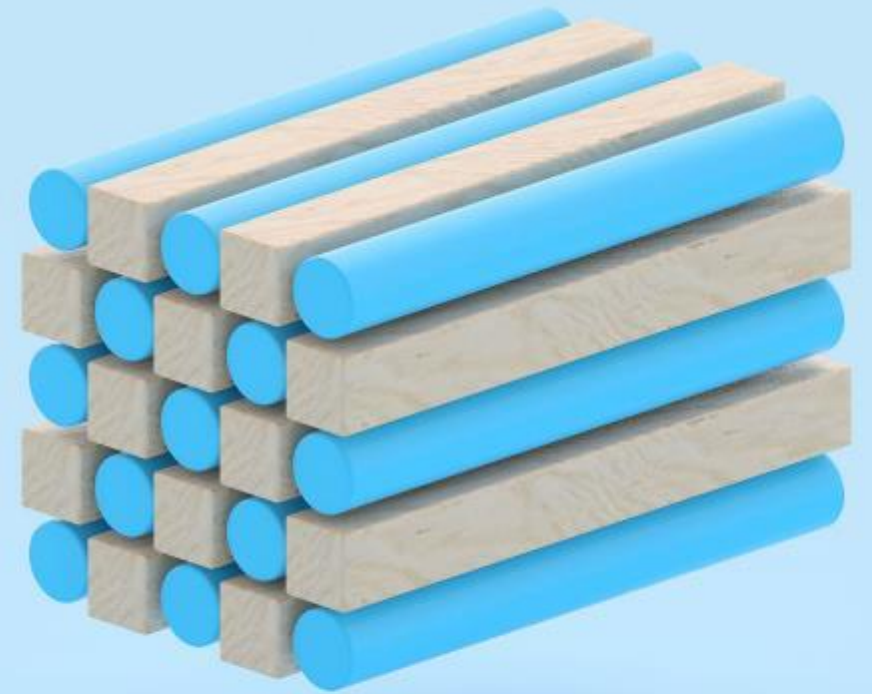
- ブラウザとリストアは、1度に最大100個のファイルをリストア可能
- 検索とリストアでは、1度に1つのファイルをリストア可能
- ファイルやフォルダのリストアは可能 (同時に最大1フォルダ)
- Archiveストレージに格納されたバックアップから、フォルダリストアは不可能

- オンプレミスからクラウドへの場合はTCOにコネクターの費用も考慮

- オンプレミスONTAPからオンプレミスのStorageGRIDの場合

- Connectorはオンプレミスで準備するとBYOLライセンスの組み合わせのみ対応

BlueXP backup and recovery コストの考え方



ライセンス情報とコストの考え方

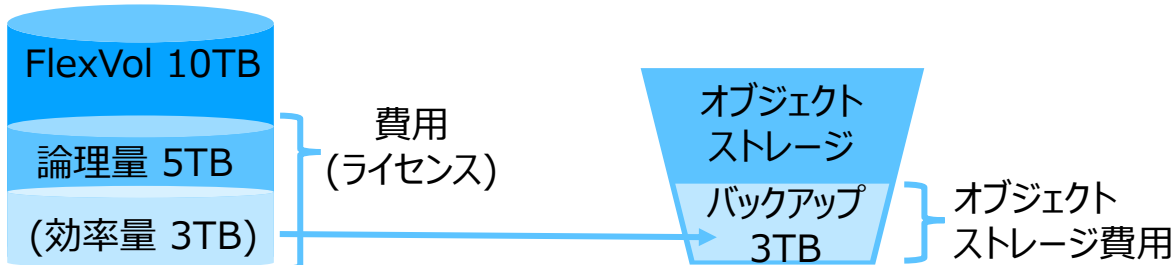
従量課金（PAYGO）、定額契約（BYOL）と両方の組み合わせ

ライセンスは2種類

- 従量課金（PAYGO）、定額契約（BYOLやマーケットプレイス）
 - 従量課金と定額契約の両方を組み合わせることが可能(定額容量を超えた場合にもサービス継続が可能)
 - オンプレのONTAPからオンプレ（StorageGRID）の場合は[BYOLのみ対応](#)
 - Cloud Volumes ONTAPで、「CVO Professional」ライセンスはクラウドバックアップを容量無制限で利用可能
 - BYOLは、合計容量がBlueXPアカウントに関連づけられた全てのシステムで共有
- NetAppの代理店からの購入やクラウドマーケットプレイスの定額契約はオンデマンドより低価格

バックアップ対象のデータ量と、バックアップの保持期間に基づく料金形態

- ONTAPのストレージ効率化機能（重複排除、圧縮等）適用前のデータ量で計算。
- バックアップデータを格納するお客様環境上のオブジェクトストレージの利用料が発生（※1）
 - ONTAPストレージ効率機能で重複排除・圧縮後されたデータで格納され、そのデータ量で費用が発生
- その他の費用：
 - NW送信（シナリオによりますが：下りトラフィック や リージョン間）（※2）
 - リストアでの料金は発生しないが、ファイル単位のリストア方法による他のクラウドサービスを利用される（※3）



Free Trial 無償 30日間 容量は無制限	PAYGO \$0.05 GB あたり 月額 クラウドプロバイダーの マーケットプレイス
--	--

12/24/36 ヶ月定額契約の場合
PAYGOより低価格
GB あたり 月額
クラウドプロバイダーのマーケットプレイス
又は BYOL

- ※1：オブジェクトストレージコストの詳細情報は[こちら](#)を参照（[AWS](#)、[Azure](#)、[GCS](#)）
- ※2：ただし、リストア時のオブジェクトストレージからのデータ取り出し費用や、データ通信費用（下りトラフィック、リージョン間）が別途発生する可能性。
- ※3：Search & Restore方法はAWSは、Amazon Athena、AWS Glue、Azureは、Azure Synapse workspace、Azure Data Lake Storage、Google CloudのBigQueryを利用します（[詳細](#)）

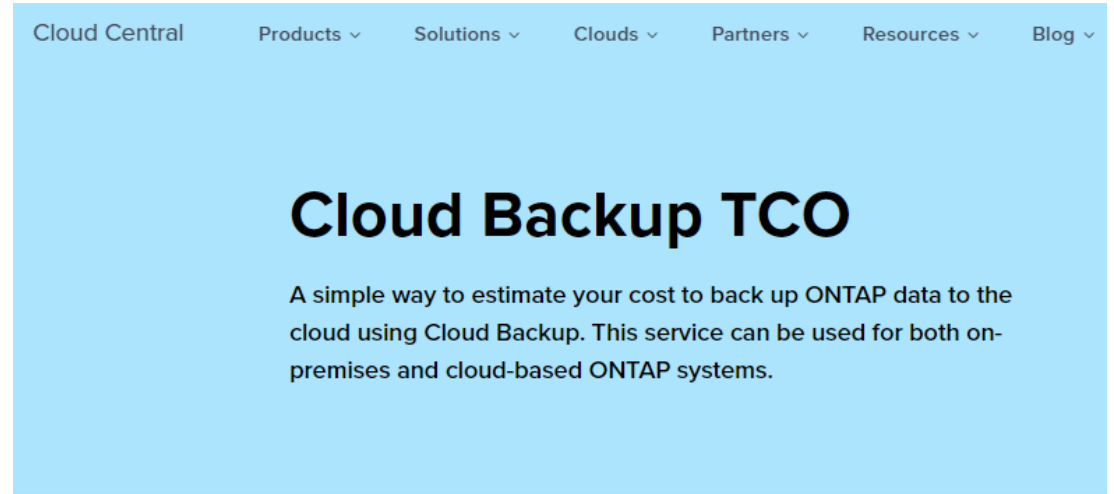


Cloud Backup TCO

“Cloud Backup TCO”を利用してクラウドバックアップを使用してONTAPデータをクラウドにバックアップするためのコストと、サードパーティベンダーに対してどのように積み重なるかを簡単に見積もり可能

このサービスは、オンプレミスとクラウドベースのONTAPシステムの両方に使用可能

[Cloud Backup TCO Calculator](#)



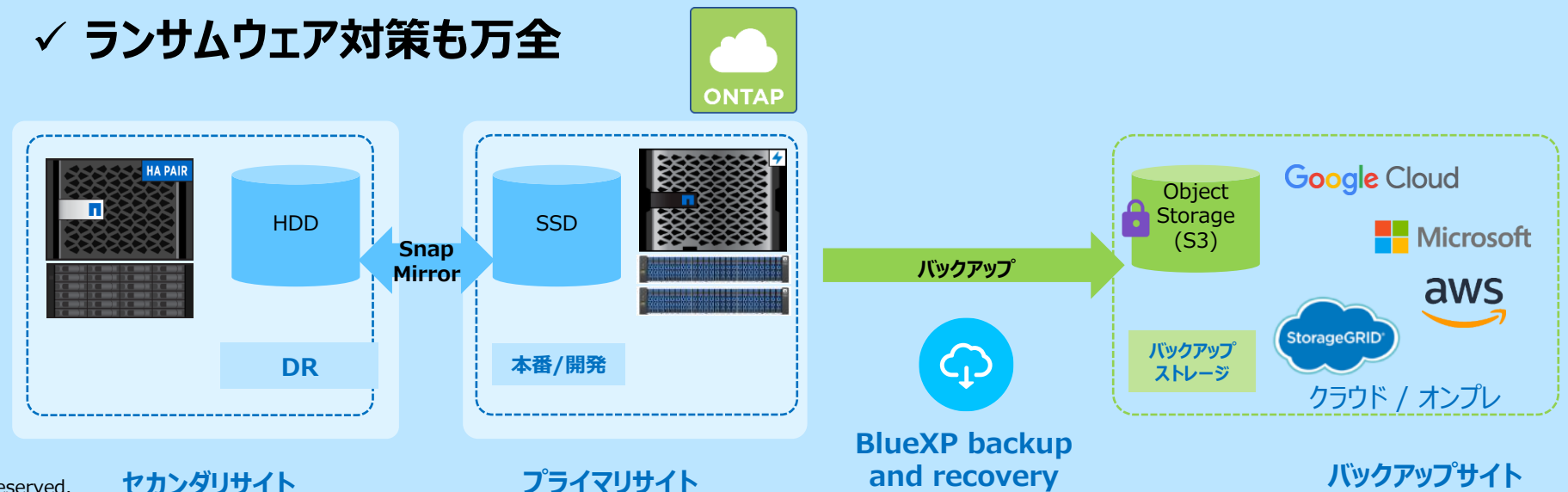
Cloud provider	aws		
Logical used capacity	100	TB	
Average storage efficiency	30	%	
Backup retention policy:			
Daily copies	30	Days	
Weekly copies	4	Weeks	
Monthly copies	12	Months	



BlueXP backup and recoveryを利用するメリット

まとめ

- ✓ 劇的にバックアップコストと管理のオーバーヘッドを減らす
- ✓ シンプルなインターフェースかつ自動化されたサービス
- ✓ RPO/RTO目標を**短期間で達成**が可能
- ✓ **信頼性、耐久性、拡張性を備えたソリューション**を展開が可能
- ✓ ネイティブのバックアップサービスとして、**統合されたUI**で操作可能
- ✓ **ランサムウェア対策も万全**



**NetApp unlocks
the best of cloud**



NetApp Tech Community ONLINE Vol.41

多様化し続けるランサムウェアもなんのその！ SB C&Sがディストリビューターとして語る 他社ベンダーにないランサムウェア対策における ネットアップの強みとは！？

ランサムウェア被害が拡大し始めて早数年。
現在も被害の数は増加傾向にあり、日々進化する攻撃手法への対策が
常に求められています。

本セッションでは、ランサムウェア被害の最新動向と他社ベンダーと比較した
ランサムウェア対策におけるネットアップの強みについて、ディストリビューターで
あるSB C&S様にご紹介いただきます。

スピーカー：
SB C&S株式会社
ICT事業本部 技術本部 第1技術部 2課
河村 龍 様



2023年6月20日（火）

16:00～16:45



ご登録：bit.ly/NTCOvol41

申込：事前登録制・無料

対象：クラウド、ITインフラ、DXに関わる企業のお客様、
パートナー様